

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

03/06/2017

SUBJECT:

Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices, including, but not limited to, smartphones, tablets, and watches. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Successful exploitation of the most severe of these vulnerabilities could result in remote code execution in the context of the application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

Android OS builds utilizing Security Patch Levels prior to March 05, 2017

RISK:

Government:

• Large and medium government entities: **High**

• Small government entities: **High**

Businesses:

• Large and medium business entities: **High**

• Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Google Android OS is prone to multiple vulnerabilities, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Remote code execution vulnerability in OpenSSL & BoringSSL (CVE-2016-2182)
- Remote code execution vulnerability in Mediaserver (CVE-2017-0466, CVE-2017-0467, CVE-2017-0468, CVE-2017-0469, CVE-2017-0470, CVE-2017-0471, CVE-2017-0472, CVE-2017-0473, CVE-2017-0474)
- Elevation of privilege vulnerability in recovery verifier (CVE-2017-0475)
- Remote code execution vulnerability in AOSP Messaging (CVE-2017-0476)
- Remote code execution vulnerability in libgdx (CVE-2017-0477)
- Remote code execution vulnerability in Framesequene library (CVE-2017-0478)
- Elevation of privilege vulnerability in Audioserver (CVE-2017-0479, CVE-2017-0480)
- Elevation of privilege vulnerability in NFC (CVE-2017-0481)
- Denial of service vulnerability in Mediaserver (CVE-2017-0482, CVE-2017-0483, CVE-2017-0484, CVE-2017-0485, CVE-2017-0486, CVE-2017-0487, CVE-2017-0488)
- Update: Denial of service vulnerability in Mediaserver (CVE-2017-0390)
- Update: Denial of service vulnerability in Mediaserver (CVE-2017-0392)
- Elevation of privilege vulnerability in Location Manager (CVE-2017-0489)
- Elevation of privilege vulnerability in Wi-Fi (CVE-2017-0490)
- Elevation of privilege vulnerability in Package Manager (CVE-2017-0491)
- Elevation of privilege vulnerability in System UI (CVE-2017-0492)
- Information disclosure vulnerability in AOSP Messaging (CVE-2017-0494)
- Information disclosure vulnerability in Mediaserver (CVE-2017-0495)
- Denial of service vulnerability in Setup Wizard (CVE-2017-0496)
- Denial of service vulnerability in Mediaserver (CVE-2017-0497)
- Denial of service vulnerability in Setup Wizard (CVE-2017-0498)
- Denial of service vulnerability in Audioserver (CVE-2017-0499)
- Elevation of privilege vulnerability in MediaTek components (CVE-2017-0500, CVE-2017-0501, CVE-2017-0502, CVE-2017-0503, CVE-2017-0504, CVE-2017-0505, CVE-2017-0506)
- Elevation of privilege vulnerability in NVIDIA GPU driver (CVE-2017-0337, CVE-2017-0338, CVE-2017-0333, CVE-2017-0306, CVE-2017-0335)
- Elevation of privilege vulnerability in kernel ION subsystem (CVE-2017-0507, CVE-2017-0508)
- Elevation of privilege vulnerability in Broadcom Wi-Fi driver (CVE-2017-0509)
- Elevation of privilege vulnerability in kernel FIQ debugger (CVE-2017-0510)
- Elevation of privilege vulnerability in Qualcomm GPU driver (CVE-2016-8479)
- Elevation of privilege vulnerability in kernel networking subsystem (CVE-2016-9806, CVE-2016-10200)
- Vulnerabilities in Qualcomm components (CVE-2016-8484, CVE-2016-8485, CVE-2016-8486, CVE-2016-8487, CVE-2016-8488)
- Elevation of privilege vulnerability in kernel networking subsystem (CVE-2016-8655, CVE-2016-9793)
- Elevation of privilege vulnerability in Qualcomm input hardware driver (CVE-2017-0516)
- Elevation of privilege vulnerability in MediaTek Hardware Sensor Driver (CVE-2017-0517)
- Elevation of privilege vulnerability in Qualcomm ADSPRPC driver (CVE-2017-0457)
- Elevation of privilege vulnerability in Qualcomm fingerprint sensor driver (CVE-2017-0518, CVE-2017-0519)
- Elevation of privilege vulnerability in Qualcomm crypto engine driver (CVE-2017-0520)
- Elevation of privilege vulnerability in Qualcomm camera driver (CVE-2017-0458, CVE-2017-0521)

- Elevation of privilege vulnerability in MediaTek APK (CVE-2017-0522)
- Elevation of privilege vulnerability in Qualcomm Wi-Fi driver (CVE-2017-0464, CVE-2017-0453, CVE-2017-0523)
- Elevation of privilege vulnerability in Synaptics touchscreen driver (CVE-2017-0524)
- Elevation of privilege vulnerability in Qualcomm IPA driver (CVE-2017-0456, CVE-2017-0525)
- Elevation of privilege vulnerability in HTC Sensor Hub Driver (CVE-2017-0526, CVE-2017-0527)
- Elevation of privilege vulnerability in NVIDIA GPU driver (CVE-2017-0307)
- Elevation of privilege vulnerability in Qualcomm networking driver (CVE-2017-0463, CVE-2017-0460)
- Elevation of privilege vulnerability in kernel security subsystem (CVE-2017-0528)
- Elevation of privilege vulnerability in Qualcomm SPCOM driver (CVE-2016-5856, CVE-2016-5857)
- Information disclosure vulnerability in kernel networking subsystem (CVE-2014-8709)
- Information disclosure vulnerability in MediaTek driver (CVE-2017-0529)
- Information disclosure vulnerability in Qualcomm bootloader (CVE-2017-0455)
- Information disclosure vulnerability in Qualcomm power driver (CVE-2016-8483)
- Information disclosure vulnerability in NVIDIA GPU driver (CVE-2017-0334, CVE-2017-0336)
- Denial of service vulnerability in kernel cryptographic subsystem (CVE-2016-8650)
- Elevation of privilege vulnerability in Qualcomm camera driver (device specific) (CVE-2016-8417)
- Information disclosure vulnerability in Qualcomm Wi-Fi driver (CVE-2017-0461, CVE-2017-0459, CVE-2017-0531)
- Information disclosure vulnerability in MediaTek video codec driver (CVE-2017-0532)
- Information disclosure vulnerability in Qualcomm video driver (CVE-2017-0533, CVE-2017-0534, CVE-2016-8416, CVE-2016-8478)
- Information disclosure vulnerability in Qualcomm camera driver (CVE-2016-8413, CVE-2016-8477)
- Information disclosure vulnerability in HTC sound codec driver (CVE-2017-0535)
- Information disclosure vulnerability in Synaptics touchscreen driver (CVE-2017-0536)
- Information disclosure vulnerability in kernel USB gadget driver (CVE-2017-0537)
- Information disclosure vulnerability in Qualcomm camera driver (CVE-2017-0452)

Successful exploitation of the most severe of these vulnerabilities could result in remote code execution in the context of the application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user to diminish the effects of a successful attack.
- Remind users to download apps only from trusted vendors in the Play Store.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Google:

<https://source.android.com/security/bulletin/2017-03-01.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8709>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2182>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5856>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5857>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8413>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8416>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8417>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8477>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8478>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8479>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8483>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8484>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8485>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8486>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8487>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8488>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8650>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8655>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9793>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9806>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10200>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0306>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0307>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0333>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0334>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0335>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0336>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0337>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0338>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0390>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0392>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0452>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0453>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0455>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0456>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0457>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0458>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0459>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0460>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0461>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0518>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0519>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0520>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0521>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0522>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0523>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0524>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0525>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0526>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0527>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0528>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0529>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0531>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0532>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0533>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0534>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0535>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0536>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0537>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>